【BSI 网络讲座】IT 治理基础-COBIT5

Q&A

1. BSI 与 ISACA 是什么关系？BSI 在 COBIT5 上提供哪些服务？

ISACA（*Information Systems Audit and Control Association* ）是 COBIT 的发布组织；BSI（英国标准协会）是国际上第一家标准研发机构，也是 ISO 的创始和重要成员。为推广 COBIT5，2012 年开始 ISACA 委托 APMG 在全球范围内代理培训课程和个人认证证书，同时 APMG 授权 BSI 开展 COBIT5 相关的培训课程和个人认证证书。

COBIT5 相关的培训课程和个人认证证书如下：

- COBIT5 基础认证课程及证书
- COBIT 5 实施课程及证书
- COBIT 5 审核员课程及证书

BSI 除提供以上标准课程之外，还提供：

- 定制化培训课程
- IT 内控审计及成熟度评估

2. COBIT5 有哪些组织已经实施？

COBIT5 是 2012 年 4 月发布的，推出时间比较短，全面实施的组织很少。相比上一版 COBIT4.1，实施的组织就比较多了。在我国，证券行业比较早就有相关的治理指引，一些券商及交易所都有相关的实施工作；此外，电力行业的一些组织也积极落实和推动 IT 治理；银行等金融行业组织，也有一些 IT 治理的相关要求。

3. COBIT5 对企业的好处？对个人的好处？

近 20 年来，IT 及通信技术在飞速发展、快速更新，造成企业不断的投资，然而投资能否产生商业价值，日益成为企业管理层面临的问题。企业的高层密切关注信息化建设与发展，希望通过有效和创新利用 IT，实现组织战略目标和商业利益，同时关注着信息技术的风险管理、IT 内部控制，优化 IT 服务和技术的成本。IT 治理帮助企业解决这些关键问题。不过，实施 IT 治理的组织，要把治理落到实处，对它原来的管理基础要求还是比较高的；我们建议实施 IT 治理的组织，应该先推行 ISO27001 和 ISO20000/ITIL，以保证实施 IT 治理取得良好的效果。

对个人来说，了解 IT 治理的理论和原则，能有效地丰富自己在 IT 治理与管理领域的知识，提高创新能力。

4. COBIT 能否与 ISO 27001 整合？

完全可以，但是要注意以下问题：

首先 COBIT 是与 ISO27001 的目的和范围均不相同的标准体系；但就组织的 IT 部门来说，COBIT 与 ISO27001 是存在交集的，完全可以整合。IT 治理的根本目的是整体提升 IT 价值，要实施 COBIT，IT 组织应该先有一个良好的管理基础，例如，成功实施了 ISO27001 和 ISO20000，在此基础上再实施 COBIT，是一种比较好的选择。

第二，COBIT5 中实施指南有一本书专门强调信息安全实施的要求，从原则来看，COBIT5 对信息安全的定义与 ISO27001 是一致的，也是从 CIA 三个方面实现信息安全，以及强调信息安全风险管理。

第三，整合 ISO27001 和 COBIT 的时候，可以以 ISO27001 为基础，从信息安全风险治理和管理领域的原则、推动力、和流程，梳理 COBIT 中信息安全要求的差距。

5. 如何进行有效的 IT 规划？

谈有效的 IT 规划，首先要明确 IT 规划的目的是什么？IT 规划的目的，大都是为了有效地控制 IT 需求并进行有效的 IT 投资决策。想清楚这个问题，如何规划就有数了。企业做 IT 规划，一个最基本的要求和出发点，就是满足业务要求，这和我们刚介绍的 COBIT5 的第一个原则是一致的。要作出令各方满意的 IT 规划，就要从他们的角度思考问题。企业的利益相关方通常有很多，而且他们的需求可能还是相互矛盾的。IT 规划，或者说 IT 治理，就是要从这些不同的需求中达成一致，IT 规划在作出利益、资源、风险等决策的时候，应充分考虑所有利益相关方的需求。对每一个决策要问清以下几个问题：

Who receives the benefits?

Who bears the risk?

What resources are required?

再有，就是要与企业业务紧密融合，在 COBIT5 中提出， IT 治理要覆盖企业端到端的业务流程和功能。IT 规划要充分了解企业的核心业务以及高优先级业务的需求。了解哪些业务在企业中起着举足轻重的作用，对业务能力和 IT 能力进行分析。业务能力分析是分析现状与企业愿景之间的差距，确定关键问题。IT 能力分析是诊断企业信息化的当前状况，分析 IT 系统对企业未来发展的适应能力，从而提出 IT 建设的方向。

6. 如何说服领导实施 COBIT？企业应如何实施 COBIT5？

COBIT5 的系列文件中一个重要的部分是 IT 治理的实施指南，并且在 COBIT5 基础框架中也有一个章节讲解实施 COBIT5 的 life cycle。这个生命周期，包括了 IT 治理实施方案的 7 个阶段、7 个变更因素及推动力，和

7 个持续改进要素；解决了为什么要 IT 治理，企业现在的水平和将要去到哪里，需要做什么，怎么达到目标的要求，测量改进的效果和如何保障持续的稳定的治理水平。

在这个 7 步方案的核心要素中，首先提到了实施 IT 治理的驱动力，这个驱动力通常包括两类：

- The enterprise specific internal and external environment factors as they apply to change management.
- The Importance of Pain Points and Trigger events that require improved governance and management of enterprise IT.

所以，说服企业领导实施 COBIT5，也要从内外部环境因素，以及企业内部痛点、关键事件出发，寻找合适的契机。